Security Notification – PowerSCADA Expert

(Wonderware ArchtestrA Logger multiple vulnerabilities)

24-August-2017

Overview

Schneider Electric® has become aware of vulnerabilities in the Wonderware ArchestrA Logger component used within the PowerSCADA Expert v8.2 product.

Vulnerability Overview

The Wonderware ArchestrA Logger component exposes a Remote Procedure Call (RPC) interface for remote management. Some of the methods on this interface are susceptible to:

- Remote Code Execution, which could allow an attacker to run arbitrary code in the context of a highly privileged account.
- Memory Leaks, which could allow an attacker to exhaust the memory of the target machine and cause Denial of Service for applications running on the target machine.
- Null Pointer Dereferences, which could allow an attacker to crash the logger process causing Denial of Service for logging and log-viewing operations.

Note that applications which use the Wonderware ArchestrA Logger continue to run when the Wonderware ArchestrA Logger service is unavailable and will function correctly, losing only the ability to log.

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

Product(s) Affected

The product(s) affected:

- PowerSCADA Expert v8.2

Vulnerability Details

The Wonderware ArchestrA Logger component exposes a Remote Procedure Call (RPC) interface for remote management. Some of the methods on this interface are susceptible to:

- Remote Code Execution, which could allow an attacker to run arbitrary code in the context of a highly privileged account.
- Memory Leaks, which could allow an attacker to exhaust the memory of the target machine and cause Denial of Service for applications running on the target machine.
- Null Pointer Dereferences, which could allow an attacker to crash the logger process causing Denial of Service for logging and log-viewing operations.

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference, they should be adapted by individual users as required.

- ArchestrA LoggerRCE
  - Overall CVSS v3 score: **9.8 (Critical)**
  - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - CVE-2017-9629
- ArchestrA LoggerLeak
  - Overall CVSS v3 score:**8.6 (High)**
  - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
  - CVE-2017-9627
- ArchestrA LoggerCrash
  - Overall CVSS v3 score: **7.5 (High)**
  - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - CVE-2017-9631

Mitigation

Schneider Electric has developed a patch which addresses the above vulnerabilities.

Download, unzip and install the patch from the following location:

- https://schneider-electric.box.com/shared/static/l21fxfghaqlzxkjt456q4gbm28qbuqyh.zip
  (SHA256 checksum to verify download of .zip file):
  C61A9164307C9B42B0A2BF318FD4442218996714188 79E1B5BEEBA91AC02BE27

Schneider Electric recommends ALL customers using the above listed affected software packages to download and apply the relevant patch.

Notes on applying the patch:

- Customers are recommended to close System Management Console (SMC) and Log Viewer applications prior to applying this patch. If the applications are open customers may receive an error. To resolve this error please restart the System Management Console (SMC) or refresh the Log Viewer applications.
- If PowerSCADA Expert v8.2 is reinstalled after this patch is applied, then the patch needs to be reinstalled after the PowerSCADA Expert v8.2 is reinstalled.

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

Schneider Electric is the global specialist in energy management and automation. With revenues of ~€25 billion in FY2016, our 160,000+ employees serve customers in over 100 countries, helping them to manage their energy and process in ways that are safe, reliable, efficient and sustainable. From the simplest of switches to complex operational systems, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2017.08.24 10:34:13 -04'00'